

**UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION**

GABRIEL PETHICK, Individually and on Behalf
of All Other Persons Similarly Situated,

Plaintiff,

v.

CHANGE HEALTHCARE INC. and
CVS PHARMACY, INC.

Defendants.

Case No.: _____

COMPLAINT – CLASS ACTION

JURY TRIAL DEMANDED

Plaintiff Gabriel Pethick (“Plaintiff”), on behalf of himself and all others similarly situated, brings this Class Action Complaint against Change Healthcare Inc. (“Change Healthcare”) and CVS Pharmacy, Inc. (“CVS”) (collectively “Defendants”). Plaintiff alleges as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to him, which are based on personal knowledge.

INTRODUCTION

1. Plaintiff brings this class action for Defendants’ failure to process pharmaceutical savings cards (“Savings Cards”) issued by drug manufacturers, pharmacies, insurance providers, non-profit organizations and healthcare companies. These Savings Cards provide consumers with substantial discounts on certain prescriptions and are crucial for patients who use them to afford necessary medications.

2. In the instant case, Plaintiff and similarly situated persons, tried to use Savings Cards but were unable to do so because of Defendants. Defendants attribute their failure to process

Savings Cards to a data breach that exploited a vulnerability in Change Healthcare's software technology, occurring around February 21, 2024 (the "Data Breach"). This breach severely compromised Change Healthcare's systems, leading to an extensive shutdown that directly impaired the Defendants' capacity to effectively manage and process Savings Cards.

3. As a direct result of the disruption, many consumers were forced to pay full price for medications they would typically purchase at a discounted rate using Savings Cards. The inability to use these Savings Cards prevented patients from accessing the discounts they were entitled to, causing financial hardship for those who use these discounts when purchasing their medications.

4. Despite knowing that they could not process Savings Cards, Defendant CVS continued to advertise the availability and benefits of these cards. When the processing system was disrupted, CVS failed to honor this commitment.

5. Additionally, despite being aware of this issue, Defendants failed to take timely measures to secure the Savings Card processing system or notify affected consumers. As a result, many consumers were not promptly informed about the problem, leaving them unaware of why their Savings Cards were not being honored and what alternative steps they could take.

6. Furthermore, Defendants failed to establish procedures to ensure the prompt processing of Savings Cards in the event of a data breach, such as implementing immediate manual processing or providing alternative solutions.

7. Importantly, Defendants failed to reimburse Plaintiff, and others similarly situated, for the discounts they were entitled to, and would have received, but for the Data Breach. Despite being aware of the systemic failures and the resulting financial impact, Defendants took no action to address the losses, leaving consumers to bear unnecessary out-of-pocket expenses.

8. The impact of the Data Breach extended to millions of consumers, forcing many to pay higher out-of-pocket costs for their prescriptions.

9. Defendants failed to credit Plaintiff's Savings Card, which entitled him to a discount of up to \$170 on each prescription for his necessary medication after an initial payment of \$25.

10. On or about March 5, 2024, Plaintiff visited a CVS Pharmacy location in Connecticut. As was customary, his Savings Card was kept on file by CVS, and he expected it to be honored and to pay only the \$25 copayment as he had done the previous month.

11. However, due to Defendants' negligence in handling the processing of Savings Cards following the Data Breach, Plaintiff was charged \$120.

12. Later that month, Plaintiff contacted CVS to dispute the charge. Instead of resolving the issue, CVS misdirected Plaintiff, instructing him to contact the drug manufacturer, who then referred him to AlphaScrip Inc. ("AlphaScrip"). AlphaScrip initially advised Plaintiff to contact his insurer, but the insurer redirected him back to AlphaScrip. After several days of repeated attempts, Plaintiff finally reached AlphaScrip again, only to be told to contact Change Healthcare. When Plaintiff contacted Change Healthcare, they, in turn, directed him back to AlphaScrip, leaving him stuck in an endless cycle of referrals, with neither CVS nor Change Healthcare resolving the issue.

13. At no point has Plaintiff been informed by Defendants of the process or timeline for receiving a refund, and to date, he has not been reimbursed for his out-of-pocket costs.

14. Plaintiff brings this Complaint on behalf of himself and all others affected by Defendants' failure to process Savings Cards during the period in which the Data Breach prevented their processing.

PARTIES

15. Plaintiff Gabriel Pethick is a resident and citizen of North Haven, Connecticut.

16. Defendant Change Healthcare is a for-profit Delaware corporation with its principal place of business at 424 Church Street, Suite 1400, Nashville, TN 37219. Change Healthcare provides payments and revenue cycle management, connecting payers, providers, and patients within the United States healthcare system. The company offers a broad range of services, including claims processing, electronic data interchange (“EDI”), and payment accuracy services, all designed to streamline operations and improve efficiency in healthcare transactions. It was acquired by UnitedHealth Group Inc. (“UHG”) in 2022 and markets itself as part of Optum, Inc. (“Optum”).

17. Defendant CVS Pharmacy is a Rhode Island corporation with its principal place of business at One CVS Drive, Woonsocket, Rhode Island 02895. CVS Pharmacy is the immediate or indirect parent of numerous pharmacy subsidiaries that own and operate pharmacies across the United States. CVS Pharmacy represents the retail arm of CVS Health Corporation (“CVS Health”) and is responsible for the sale of prescription drugs, over-the-counter medications, health and wellness products, and other retail items. It serves as the face of the company to millions of consumers who visit its physical stores. As of May 2024, CVS Pharmacy operates 9,160 locations across all 50 states, including 139 locations across Tennessee. Additionally, CVS Pharmacy engages in marketing, advertising, and promotional activities within Tennessee to drive traffic to these stores and to its online platforms. Moreover, CVS Pharmacy participates in state-specific healthcare initiatives, collaborates with Tennessee healthcare providers, and contracts with local businesses and government entities in Tennessee.

JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of \$5,000,000, there are more than 100 proposed Class Members, and minimal diversity exists, as all Defendants are citizens of a State different from that of at least one Class member (i.e., Plaintiff). This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

19. This Court has personal jurisdiction over Defendants because Change Healthcare's principal place of business is in Nashville, Tennessee, within this District; each defendant is authorized to, and regularly conducts business in, the State of Tennessee; and each defendant intentionally avails themselves of Tennessee's markets by selling, marketing, and advertising its products and services to Class Members located in the State of Tennessee and within this District. Defendants therefore have sufficient minimum contacts to render the exercise of jurisdiction by this Court proper and necessary.

20. Venue is proper in this District pursuant to 28 U.S.C. § 1391(a) through (d) because Change Healthcare's principal place of business is located in this District, and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in, was directed to, and/or emanated from this District.

FACTUAL ALLEGATIONS

I. Change Healthcare's Role in Pharmacy Billing and Transactions

21. Change Healthcare is a major healthcare technology firm in the U.S., specializing in enhancing clinical, administrative, and financial processes for payers, providers, and consumers. Its services include claims processing, insurance verification, payment disbursement, and

authorization reviews, which are accessed by providers either through direct contracts or third-party intermediaries.

22. According to the Change Healthcare website, its “extensive network, innovative technology, and expertise inspire a stronger, better coordinated, increasingly collaborative, and more efficient healthcare system.”¹ It bills itself as a “trusted partner for organizations committed to improving the healthcare system through technology.”²

23. Change Healthcare markets its suite of pharmacy solutions as tools to “simplify pharmacy billing and improve revenue cycle with tools for third-party submission and reconciliation, outsourced ‘chasing claims,’ contract management, appeal submission, and tracking services.”³ The company asserts that its offerings “help you improve claims management, audit and appeal processes, and take advantage of enhanced billing practices to boost revenues.”⁴

24. Change Healthcare also represents to providers that its “advanced technology and services help . . . enhance patient engagement and access, improve outcomes, drive revenue performance, and improve operational efficiency.” Change Healthcare further asserts that its solutions help payers meet their priorities throughout the member journey, empower partners to achieve strategic business objectives, and satisfy customer needs. Additionally, Change Healthcare assures patients that its solutions streamline the engagement, care, and payment experience to “improve the patient journey.”⁵

¹ <https://www.changehealthcare.com/> (last visited September 18, 2024).

² <https://cs-gw-www.dev.changehealthcare.com/> (last visited September 18, 2024).

³ <https://www.changehealthcare.com/pharmacy> (last visited September 18, 2024).

⁴ *Id.*

⁵ <https://www.changehealthcare.com/> (last visited September 18, 2024).

25. Change Healthcare is the nation's largest clearinghouse for insurance claims and payments, connecting over 800,000 healthcare providers and 2,100 payers.⁶ It connects with one in every three patient records in the U.S. and processes 15 billion healthcare transactions annually.⁷

26. In its role as a clearinghouse, Change Healthcare is responsible for processing patient payments on behalf of pharmacies, including CVS. This includes handling claims, reimbursements, and the processing of Savings Cards and patient assistance programs.

27. When a patient has a prescription filled at CVS, the pharmacy submits a claim to Change Healthcare. Change Healthcare reviews these claims for accuracy and compliance with payer requirements before processing them. Once processed, the claim is sent to the insurer or payer, who then determines whether to approve or deny the payment. If approved, the payer issues payment to the pharmacy along with a Remittance Advice or Explanation of Benefits, which details the amount paid and any adjustments. CVS uses this information to reconcile the patient's account and ensure that any discounts, such as those from Savings Cards, are properly applied.

28. Additionally, Change Healthcare's platform processes a substantial portion of insurance claims, including those managed by Aetna, which is owned by CVS Health.

29. Given the breadth of Change Healthcare's network and its central role in this process, any disruption to their platform can significantly interrupt the ability of pharmacies to process claims and receive payments, thereby affecting the entire billing cycle.

30. In 2021, UHG proposed a deal to acquire Change Healthcare for approximately \$13 billion, including debt. The acquisition was aimed at merging Change Healthcare with Optum, Inc.

⁶ <https://www.changehealthcare.com/medical-network/claiming-remittance> (last visited September 18, 2024).

⁷ Richard J. Pollack, *AHA Letter to HHS on Implications of Change Healthcare Cyberattack* (February 26, 2024) <https://www.aha.org/lettercomment/2024-02-26-aha-letter-hhs-implications-change-healthcare-cyberattack> (last visited September 18, 2024).

(“Optum”), a subsidiary of UHG that provides technology services, pharmacy care services, and various direct healthcare services.

31. In a January 6, 2021 press release announcing the merger agreement, Andrew Witty, President of UHG and CEO of Optum, stated that “[t]ogether we will help streamline and inform the vital clinical, administrative and payment processes on which health care providers and payers depend to serve patients.”⁸

32. Melinda Reid Hatton, American Hospital Association (“AHA”) Vice President and General Counsel, voiced concerns about the proposed deal and wrote to the Department of Justice (“DOJ”) asking it to investigate the potential merger. In the letter to the DOJ, Ms. Hatton wrote, “The proposed acquisition would produce a massive consolidation of competitively sensitive healthcare data and shift such data from Change Healthcare, a neutral third party, to Optum.”⁹

33. The DOJ initially filed a lawsuit to block the merger of Change Healthcare and Optum, citing antitrust concerns.¹⁰ In its complaint, the DOJ described Change Healthcare as a technology company that operates “the nation’s largest electronic data interchange (“EDI”) clearinghouse, which transmits data between healthcare providers and insurers, allowing them to exchange insurance claims, remittances, and other healthcare-related transactions . . . It has access to a vast trove of competitively sensitive claims data that flows through its EDI clearinghouse—over a decade’s worth of historic data as well as billions of new claims each year.”¹¹ Moreover,

⁸ *OptumInsight and Change Healthcare Combine to Advance a More Modern, Information and Technology-Enabled Health Care Platform* (January 6, 2021) <https://www.sec.gov/Archives/edgar/data/1756497/000119312521002414/d40030dex991.htm> (last visited September 18, 2024).

⁹ <https://www.aha.org/system/files/media/file/2021/03/aha-urges-doj-investigate-unitedhealth-groups-acquisition-change-healthcare-letter-3-18-21.pdf> (last visited September 18, 2024).

¹⁰ <https://www.justice.gov/opa/pr/justice-department-sues-block-unitedhealth-group-s-acquisition-change-healthcare> (last visited September 18, 2024).

¹¹ See <https://www.justice.gov/atr/case-document/file/1476901/dl> (last visited September 18, 2024).

according to the DOJ, “50 percent of all medical claims in the United States pass through Change’s EDI clearinghouse.”¹²

34. The DOJ, however, lost its challenge to UHG’s acquisition of Change Healthcare after a district judge ruled in UHG’s favor and the DOJ chose not to appeal, and on October 2022 Optum completed its combination with Change Healthcare.

II. The Impact of the Data Breach on Patients’ Access to Savings Card Processing

35. On February 12, 2024, hackers infiltrated Change Healthcare’s systems through a vulnerability in the company’s remote login application, known as the Change Healthcare Citrix portal. This portal lacked multi-factor authentication, which is data security 101, allowing unauthorized access using login credentials. This significant security lapse enabled hackers to penetrate Change Healthcare’s network without additional identity verification. For at least a week, the breach went unnoticed. During this period, hackers moved laterally within the system, exfiltrating data and installing ransomware.¹³ This unauthorized access allowed them to launch a large-scale ransomware attack.

36. On or about February 21, 2024, Defendants discovered the Data Breach and that their computer networks were not secure and could not protect personal health information (“PHI”) and personally identifiable information (“PII”). UHG set up a website at www.unitedhealthgroup.com to announce the Data Breach and stated that it had disconnected the Change Healthcare systems. UHG also stated, “The Company has retained leading security experts, is working with law enforcement and notified consumers, clients and certain government

¹² *Id.*

¹³ Testimony of Andrew Witty, Chief Executive Officer, UnitedHealth Group, Before the House Energy and Commerce Committee Subcommittee on Oversight and Investigations “Examining the Change Healthcare Cyberattack,” https://www.finance.senate.gov/imo/media/doc/0501_witty_testimony.pdf (May 1, 2024) (last visited September 18, 2024).

agencies . . . At this time, the Company believes the network interruption is specific to Change Healthcare systems, and all other systems across the Company are operational.”¹⁴

37. In response to the Data Breach, on February 24, 2024, the AHA issued a cybersecurity advisory, recommending that “all healthcare organizations that were disrupted or are potentially exposed by this incident consider disconnection from” the affected Change Healthcare applications.¹⁵ The AHA stated that, **“As of this date, Change Healthcare has not provided a specific timeframe for which recovery of the impacted applications is expected.”**¹⁶

38. On February 28, 2024, the cybercriminal group ALPHV/BlackCat claimed responsibility for the attack.¹⁷ The group has been in operation since November 2021 and had been the subject of various warnings from government authorities. The Data Breach was consistent with the group’s widely-reported past operations.

39. When ALPHV/BlackCat publicized the breach on its dark web site on February 28, 2024, it also accused UHG of misleading the public about the severity and scope of the incident. The group warned UHG that it was “walking on a very thin line.”¹⁸

40. The stolen data included millions of medical and dental records, insurance details, payment information, contact information, military records, Social Security numbers, and over 3,000 source code files for Change Healthcare solutions.¹⁹

¹⁴ UHG Form 8-K (February 22, 2024), <https://www.sec.gov/Archives/edgar/data/731766/000073176624000045/unh-20240221.htm> (last visited September 18, 2024).

¹⁵ <https://www.aha.org/2024-02-24-update-unitedhealth-groups-change-healthcares-continued-cyberattack-impacting-health-care-providers> (last visited September 18, 2024).

¹⁶ *Id.* (emphasis in original).

¹⁷ Bradford Regeski, *BlackCat/ALPHV Claims Responsibility for Change Healthcare Ransom*, RH-ISAC (Feb. 28, 2024), <https://rhisac.org/threat-intelligence/blackcat-alphv-claims-responsibility-for-change-healthcare-ransom/> (last visited September 18, 2024).

¹⁸ Brett Callow – X, Twitter Post with Screenshot, <https://twitter.com/BrettCallow/status/1762893128326111404> (Feb. 28, 2024) (last visited September 18, 2024).

¹⁹ *Id.*

41. At the May 1, 2024 Subcommittee on Oversight and Investigation Hearing, UHG CEO Andrew Witty estimated that one-third of Americans were impacted by the Data Breach.²⁰

42. UHG later admitted that it paid a ransom to ALPHV/BlackCat, which many reports suggest was for 350 Bitcoin, or approximately \$22 million.²¹

43. This is not the first time that UHG has dealt with a data breach. In December 2023, OptumRx, a UHG subsidiary, announced that some patients' personal information was exposed in a major cyberattack.²² Additionally, in May 2023, United Healthcare Inc. ("United Healthcare"), also a UHG subsidiary, had to notify members that protected health information may have been compromised due to a credential stuffing attack that occurred on the United Healthcare mobile app in February 2023.²³

44. On March 13, 2024, the AHA wrote to Senators Ron Wyden and Mike Crapo about the Data Breach. According to the AHA's letter, the downed systems "are hampering providers' ability to verify patients' health insurance coverage, process claims and receive payment from many payers, exchange clinical records with other providers, provide cost estimates and bill patients, and in some instances, access the clinical guidelines used in clinical decision support tools and as part of the prior authorization process."²⁴

²⁰ Ashley Capoot, *UnitedHealth CEO estimates one-third of Americans could be impacted by Change Healthcare cyberattack* (May 20, 2024), <https://www.cnn.com/2024/05/01/unitedhealth-ceo-one-third-of-americans-could-be-impacted-by-change-healthcare-cyberattack.html?os=io.&msockid=3966bcd438936e4526cdad4f391c6ff1> (last visited September 18, 2024).

²¹ Testimony of Andrew Witty, Chief Executive Officer, UnitedHealth Group, Before the House Energy and Commerce Committee Subcommittee on Oversight and Investigations "Examining the Change Healthcare Cyberattack," https://www.finance.senate.gov/imo/media/doc/0501_witty_testimony.pdf (May 1, 2024) (last visited September 18, 2024); Ashley Capoot, *UnitedHealth CEO tells lawmakers the company paid hackers a \$22 million ransom* (May 1, 2024), <https://www.cnn.com/2024/05/01/unitedhealth-ceo-says-company-paid-hackers-22-million-ransom.html> (last visited September 18, 2024).

²² <https://www.kplctv.com/2023/12/21/optumrx-patients-data-compromised-data-breach/> (last visited September 18, 2024).

²³ <https://www.cbsnews.com/losangeles/news/united-healthcare-reports-data-breach-that-may-have-revealed-customers-personal-information/> (last visited September 18, 2024).

²⁴ <https://www.aha.org/system/files/media/file/2024/03/Letter-AHA-Urges-Congress-to-Provide-Support-to-Help-Minimize-Further-Fallout-from-Change-Healthcare-Attack.pdf> (last visited September 18, 2024).

45. The Data Breach had significant repercussions for pharmacies across the United States. On February 21, 2024, Change Healthcare took its systems offline and issued a vague statement, indicating they were unable to predict the “duration or extent of the disruption.”²⁵

46. This lack of preparedness directly impacted CVS, which relied heavily on Change Healthcare’s systems to process payments through patients’ healthcare plans. Both Change Healthcare and CVS failed to ensure a reliable backup plan, leading to a breakdown in service delivery. By failing to maintain continuity in their operations, both companies bear responsibility for the ensuing chaos that left patients unable to use their Savings Cards.

47. In a statement to CNBC, CVS Health acknowledged that the disruption had impacted some of its business operations including the inability to process insurance claims.²⁶ However, CVS made no mention of the impact on Savings Cards or any efforts to help patients who relied on these cards for necessary discounts.

48. On February 28, 2024, Patrick Conway, CEO of OptumRx, a subsidiary of UHG and a division of Optum, issued a letter to pharmacy partners stating:

On a call with multiple pharmacy association partners yesterday, Optum Rx committed to reimbursing all claims that are appropriate and filled with the good faith understanding that a medication should be covered. Optum Rx will take a reasonable approach to our claims reviews and audits for claims during this period, given these extraordinary circumstances and understanding the limited information that may be available to certain network pharmacies processing prescriptions during the outage.²⁷

49. On March 1, 2024, the National Community Pharmacists Association (“NCPA”), American Pharmacists Association (“APhA”), National Alliance of State Pharmacy Associations

²⁵ UHG Form 8-K (February 22, 2024) <https://www.sec.gov/Archives/edgar/data/731766/000073176624000045/unh-20240221.htm> (last visited September 18, 2024).

²⁶ <https://www.cnbc.com/2024/02/27/unitedhealths-change-healthcare-cyberattack-outages-continue-pharmacies-deploy-workarounds.html> (last visited September 18, 2024).

²⁷ <https://ncpa.org/sites/default/files/2024-02/pconway-letter-network-pharmacy-partners.pdf> (last visited September 18, 2024).

(“NASPA”), and The American Society of Consultant Pharmacists (“ASCP”) authored an open letter to Pharmacy Benefit Manager (“PBM”) executives. The letter suggested that PBMs, such as OptumRx, declare a payer-recognized emergency for claims affected by the outage. Specifically, the letter requested that “[i]f a pharmacy filled a new prescription and the patient paid out-of-pocket (assuming deductible phase due to first quarter timing of this incident), please provide instructions to patients for the plan to reimburse the patient.”²⁸

50. Despite these assurances and requests, reimbursements to consumers with Savings Cards who paid out-of-pocket for their medications during the system outage caused by the Data Breach remain unpaid.

51. Savings Cards, which offer discounts on prescription medications, are provided by state governments, drug companies, and various businesses, both non-profit and for-profit. Some of these cards are free, while others require registration or a fee. For many consumers, these cards are essential for affording their medications.²⁹

52. Typically, Savings Card providers enter into agreements with pharmacies to provide discounts to consumers who are utilizing the card, and then charge a fee per transaction. When a patient presents a Savings Card at CVS, the pharmacy enters the card information into its system, which then communicates with Change Healthcare to verify the card’s validity and calculate the discount.

53. Change Healthcare processes the transaction by submitting a claim to the payer (either the insurance company or Savings Card program administrator). Change Healthcare is tasked with ensuring that the discount is accurately applied and that CVS is reimbursed for the

²⁸ <https://www.pharmacist.com/Pharmacy-open-letter-to-PBM-Executives> (last visited September 18, 2024).

²⁹ <https://www.needymeds.org/ddc-faq> (last visited September 18, 2024).

discount extended to the patient, with funds usually provided by the pharmaceutical company or Savings Card issuer as part of their patient assistance program.

54. CVS's primary role is to accept the Savings Card, apply the discount at the point of sale, and submit the transaction for processing, while Change Healthcare serves as the intermediary, managing the claims process, verifying discounts, and coordinating communication between CVS, the insurance payer, and the Savings Card issuer.

55. Due to the Data Breach and subsequent system outage, many consumers were unable to use their Savings Cards. This forced them to pay out-of-pocket for expensive prescription drugs, leading to significant financial strain.³⁰

III. Defendants Inadequate Contingency Planning for Savings Card Processing During and After the Data Breach

56. The healthcare industry is a well-known target for cybercriminals because of the sheer volume of highly sensitive personal data stored on their systems. Consequently, healthcare providers are expected to have robust contingency measures in place not only to prevent such attacks but also to ensure that critical services continue uninterrupted in the event of a breach.

57. Despite this known risk, Change Healthcare and CVS failed to implement adequate contingency measures to ensure the continued processing of Savings Cards during the Data Breach. This oversight resulted in significant out-of-pocket expenses for consumers who use these discounts to afford their medications.

58. The prevalence of data breaches and identity theft has increased dramatically in recent years, particularly in the healthcare sector. In the first half of 2022 alone, the healthcare

³⁰ <https://www.washingtonpost.com/wellness/2024/03/05/change-healthcare-hack-prescriptions-affect/> (last visited September 18, 2024).

sector experienced about 337 breaches, with nearly 80% of incidents attributed to malicious activity.³¹

59. BlackCat/ALPHV is a well-known group of cybercriminals with a history of targeting health industry organizations. In April 2022, the Federal Bureau of Investigation (“FBI”) issued a Flash alert, designed to help cybersecurity professionals and system administrators guard against malicious actions of cybercriminals, specifically on BlackCat/ALPHV.³² In December 2023, the FBI, the Cybersecurity and Infrastructure Security Agency (“CISA”), and the Department of Health and Human Services (“HHS”) updated this alert with a joint advisory released on December 19, 2023, following a BlackCat/ALPHV administrator’s post to its affiliates encouraging them to target hospitals in December 2023. The advisory stated that “[s]ince mid-December 2023, of the nearly 70 leaked victims, the healthcare sector has been the most commonly victimized . . . FBI, CISA, and HHS encourage critical infrastructure organizations to implement the recommendations in the Mitigations section of this [Cybersecurity Advisory] to reduce the likelihood and impact of ALPHV Blackcat ransomware and data extortion incidents.”³³

60. Even prior to the FBI’s updated advisory, Change Healthcare was aware of this concerning trend, acknowledging that: “In recent years, there have been a number of well-publicized data breaches involving the improper dissemination of personal information of individuals both within and outside of the healthcare industry.”³⁴

³¹ <https://www.techtarget.com/healthtechsecurity/news/366594713/Health-Sector-Suffered-337-Healthcare-Data-Breaches-in-First-Half-of-Year> (last visited September 18, 2024).

³² FBI, BlackCat/ALPHV Ransomware Indicators of Compromise, FBI Cyber Division (Apr. 19, 2022), <https://www.ic3.gov/Media/News/2022/220420.pdf> (last visited September 18, 2024).

³³ Cybersec. & Infrastructure Sec. Agency, #StopRansomware: ALPHV Blackcat (Dec. 19, 2023), <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a> (last visited September 18, 2024).

³⁴ Change Healthcare, Amendment No. 1 to Form S-1 Registration Statement, filed June, 14, 2019 at p. 34. <https://www.sec.gov/Archives/edgar/data/1756497/000095012318012316/filename1.htm> (last visited September 18, 2024).

61. Change Healthcare was also aware that its infrastructure, data, and business operation systems experience unauthorized access of confidential information from time to time, stating:

Because our products and services involve the storage, use and transmission of personal information of consumers, we and other industry participants have been and expect to routinely be the target of attempted cyber and other security threats by outside third parties, including technically sophisticated and well-resourced bad actors attempting to access or steal the data we store.³⁵

62. Similarly, CVS acknowledged in its 2023 Impact Report, titled “Healthy 2030,” that data security, privacy and cybersecurity are top priorities. The report emphasized: “Our robust cybersecurity program enables business resiliency. We continuously monitor our third parties’ ability to deliver services securely, and we are building zero trust principles into our operating models.”³⁶

63. The Health Insurance Portability and Accountability Act (“HIPAA”) and Health Information Technology for Economic and Clinical Health Act (“HITECH”) impose strict requirements on healthcare organizations to establish and maintain contingency plans to ensure the availability, integrity, and confidentiality of electronic protected health information (“ePHI”) in the event of a data breach or similar incident.

64. The regulations under HIPAA’s Security Rule specifically require an Emergency Mode Operation Plan (45 CFR § 164.308(a)(7)(ii)(C)) to ensure the continuity of critical functions related to ePHI during emergencies like a data breach.

65. While HIPAA primarily focuses on the protection of ePHI, the operational scope of both Change Healthcare and CVS extends beyond just ePHI. Their responsibilities include the

³⁵ *Id.* at 42.

³⁶ <https://www.cvshealth.com/content/dam/enterprise/cvs-enterprise/pdfs/2023/Healthy-2030-Impact-Report-Appendix.pdf> (last visited September 18, 2024).

processing of claims, payment transactions, and Savings Cards. Given the critical nature of these services, their contingency planning should have been comprehensive, ensuring the continuity of these essential functions even in the event of a system compromise. This includes having strategies in place to maintain crucial operations, such as the processing of Savings Cards, even if primary systems are compromised.

66. However, instead of implementing robust contingency measures, Change Healthcare opted to take its systems completely offline without deploying alternative solutions. They failed to implement strategies like transitioning to backup systems, adopting manual processing methods, or establishing partnerships with third-party service providers that could have ensured the continuity of these critical services during the outage.

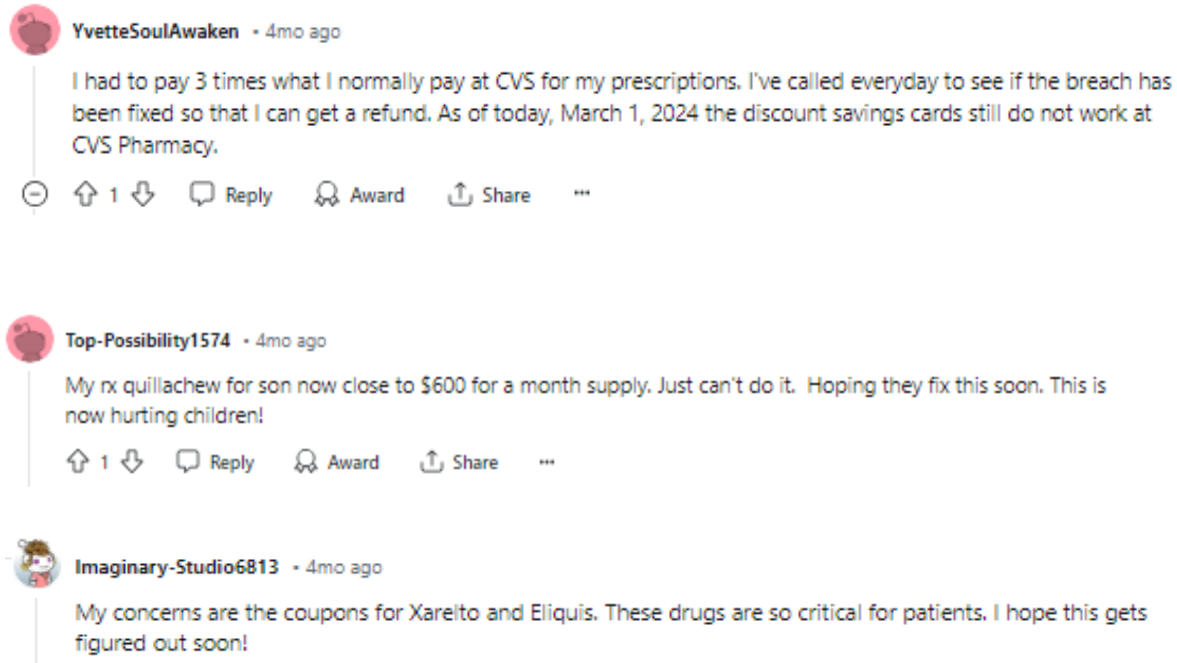
67. Similarly, CVS did not anticipate the potential downtime of Change Healthcare's systems and failed to establish contingency procedures to ensure the continuity of Savings Card processing. As a result, when Change Healthcare's servers went down, CVS was unable to process the discounts provided by Savings Cards. Consequently, consumers were forced to pay higher out-of-pocket costs for their medications because the discounts could not be applied.

68. Even as some systems were restored, CVS remained unable to process Savings Cards. This ongoing issue further exacerbated the financial burden on consumers, who continued to face increased costs due to the inability of CVS to apply the discounts.

69. A March 5, 2024, article in the *Washington Post* highlighted a customer who encountered significant difficulties obtaining her medication due to the Data Breach. Initially, she was informed that her medication would cost \$1,700 for a four-week supply because the system outage prevented her insurance from being processed. Although her insurance was eventually restored, she was still waiting for her Savings Card to be accepted. Without the Savings Card, her

medication would cost \$450 per month, whereas the Savings Card reduces the price to just \$15 per month.³⁷

70. Many affected consumers turned to the internet to express their concerns and seek advice. For example, numerous consumers posted on Reddit to share their experiences and frustrations:



71. Additionally, the Defendants failed to establish clear communication protocols to inform consumers and healthcare providers that Savings Cards would not be processed during the Data Breach, leaving many in the dark and worsening the financial burden on affected consumers.

72. Change Healthcare did not begin the process of notifying affected entities until June 2024, several months after the Data Breach was initially discovered. Change Healthcare stated that it had completed the review of over 90% of impacted files by late June but only started mailing

³⁷ <https://www.washingtonpost.com/wellness/2024/03/05/change-healthcare-hack-prescriptions-affect/> (last visited September 18, 2024).

individual breach notifications in late July.³⁸ However, these notifications focused solely on compromised data and did not address the impact on the processing of Savings Cards. As a result, many consumers were left unaware of the specific disruptions to their ability to use Savings Cards, only discovering the issue when they visited CVS and were informed at the counter.

73. Similarly, CVS failed to notify consumers about the impact of the Data Breach. In its 10-Q for the quarter ending March 31, 2024, filed on May 1, 2024, CVS Health reported only that “[v]isibility across the health insurance industry was significantly impaired by the cyberattack on Change Healthcare during the first quarter of 2024, which resulted in delayed receipt and processing of claims.”³⁹ However, CVS did not mention how the breach would affect the use of Savings Cards. Consumers only became aware of the issue when they attempted to fill their prescriptions and were informed at the pharmacy that the Savings Cards could not be processed.

74. The delayed notifications from both Change Healthcare and CVS drew sharp criticism from regulatory bodies and industry associations. The HHS noted that while covered entities could delegate breach notification duties to Change Healthcare, this delegation required proper communication and coordination. The resulting communication failures led to widespread confusion and frustration, with healthcare providers struggling to manage the situation and consumers often unaware of the breach until they faced unexpected out-of-pocket expenses at the pharmacy.⁴⁰

IV. Defendants’ Failure to Process Savings Cards Caused Harm to Plaintiff and Class Members

³⁸ <https://healthitsecurity.com/news/change-healthcare-begins-data-breach-notification-process> (last visited September 18, 2024).

³⁹ Quarterly report for quarter ending March 31, 2024, filed May 1, 2024 at p.43. https://s2.q4cdn.com/447711729/files/doc_financials/2024/q1/Q1-2024-Form-10-Q.pdf (last visited September 18, 2024).

⁴⁰ <https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/> (last visited September 18, 2024).

75. Plaintiff Pethick obtained his Savings Card directly from the drug manufacturer and has successfully used it for at least seven years, most recently on April 2, 2024. This Savings Card program is designed to reduce prescription costs and has been consistently honored by various pharmacies, including CVS Pharmacy.

76. While there may be slight variations in the terms of different Savings Cards, they uniformly impose specific obligations on both the user and the pharmacy. These terms typically require that “the patient agrees to report their use of this offer to any third party that reimburses or pays for any part of the prescription price.” They also generally include provisions stating that “participating patients, pharmacies, physician offices, and hospitals are obligated to inform third-party payers about the use of the offer as provided for under the applicable insurance or as otherwise required by contract or law.” By participating in this program and regularly honoring the Savings Card, CVS Pharmacy effectively accepted these terms and was contractually obligated to adhere to them.

77. On or about March 4, 2024, Plaintiff received a text message from CVS notifying him that his prescription would be available for pickup that day at the CVS Pharmacy located at 660 Foxon Road, East Haven, Connecticut. Plaintiff immediately checked his CVS online account and was notified that the outstanding co-payment was \$120, rather than the expected \$25 copayment using his Savings Card, in accordance with the terms of the Savings Card program.

78. Plaintiff’s expectation was founded not only on the terms and conditions of the Savings Card program but also on CVS Pharmacy’s consistent and longstanding practice of honoring the Savings Card. Through repeated use and CVS’s continued acceptance of the Savings Card, a reasonable expectation was created that CVS would persist in honoring the card under the same conditions. This consistent practice, coupled with CVS’s ongoing promotion of the Savings

Card program, established an implied contractual obligation for CVS to continue honoring the Savings Card, which CVS reinforced by their actions and marketing efforts.

79. CVS publicly positions itself as a champion of affordable healthcare, asserting a strong commitment to making prescriptions more affordable for its consumers. This commitment is highlighted through CVS's efforts to lower out-of-pocket costs using proprietary tools designed to search for discounts and identify savings opportunities. CVS claims that its pharmacy teams routinely conduct prescription savings reviews, leveraging these tools to find applicable coupons, check insurance coverage, and explore lower-cost alternatives for patients.⁴¹

80. CVS markets its commitment to affordability by claiming that "85% of CVS prescriptions are under \$10 per month." CVS promotes its ability to search across third-party discount programs, even for customers without a CVS.com account.⁴²

81. Furthermore, CVS's own website explicitly states that they accept Savings Cards for a wide range of prescription medications, further reinforcing the Plaintiff's reasonable expectation that his Savings Card would be accepted. The CVS Cash Discount Tool, available on their website, lists a long selection of drugs for which CVS pharmacies accept Savings Cards and other discounts, thereby promoting these benefits as readily available to consumers.⁴³ By making these representations, CVS creates an implied contractual obligation to uphold the terms advertised, as consumers reasonably anticipate that their Savings Cards will be honored when choosing to fill prescriptions at CVS.

82. The value of these Savings Cards cannot be overstated. In a survey of U.S. adults aged 65 and older, 30% of respondents reported using a Savings Card when obtaining their

⁴¹ <https://www.cvshealth.com/services/pharmacy/prescription-drug-savings.html> (last visited September 18, 2024).

⁴² <https://www.cvs.com/content/prescription-savings> (last visited September 18, 2024).

⁴³ <https://www.cvs.com/pharmacy/cash-discount-tool/#/drugsearch> (last visited September 18, 2024).

medications.⁴⁴ Another survey conducted by the Massachusetts Health Policy Commission (“HPC”) indicated that while branded drugs make up only 10% of prescriptions dispensed in the U.S., they account for 79% of total drug spending—largely driven by the use of Savings Cards and other incentives that encourage the purchase of more expensive branded medications.⁴⁵ The availability and acceptance of such discounts significantly influence where consumers choose to fill their prescriptions. Pharmacies that advertise their acceptance of these Savings Cards often gain a competitive advantage, attracting customers who might otherwise choose a different pharmacy.

83. On March 5, 2024, Plaintiff visited the same CVS Pharmacy and informed the pharmacist that the outstanding balance was incorrect and that his Savings Card had not been applied. The pharmacist informed Plaintiff that the Savings Card could not be processed due to an ongoing outage with Change Healthcare’s systems.

84. Requiring immediate access to his medication, Plaintiff paid the \$120 owed, anticipating that he would be refunded the \$95 difference once systems were restored.

85. Later that month, on March 23, 2024, Plaintiff returned to the same CVS Pharmacy and inquired with the pharmacist about information for consumers who lost money due to the inability to process Savings Cards. The pharmacist advised Plaintiff to contact CVS customer service.

86. On or about March 27, 2024, Plaintiff made three phone calls to CVS customer service, spending approximately 43 minutes on the phone. Despite his efforts, he was ultimately directed to contact the drug manufacturer that had issued the Savings Card.

⁴⁴ <https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2805012> (last visited September 18, 2024).

⁴⁵ Prescription Drug Coupon Study, Report to the Massachusetts Legislature (July 2020) <https://www.mass.gov/doc/prescription-drug-coupon-study/download> (last visited September 18, 2024).

87. On or about March 29, 2024, Plaintiff called the Savings Card issuer and was advised to contact the manufacturers' coupon rebate facilitator: AlphaScrip.

88. AlphaScrip is responsible for processing manufacturers' coupons on behalf of drug manufacturers and paying the proceeds obtained from the manufacturers to pharmacies that were able to submit the manufacturers' coupon.

89. When Plaintiff contacted AlphaScrip, he was told to call his insurance company, Aetna.

90. On the same day, Plaintiff called Aetna and spoke with a representative for 15 minutes, but they informed him that they had no involvement with the processing of Savings Cards.

91. On April 2, 2024, Plaintiff visited CVS Pharmacy to refill his prescription. By this time, Change Healthcare's systems had been restored, and Plaintiff's Savings Card was successfully processed.

92. Beginning April 2, 2024, Plaintiff made repeated attempts to reach AlphaScrip. After persistent efforts through the first week of April, Plaintiff finally connected with a representative on April 5, 2024, who referred him to the Change Healthcare Pharmacy Helpdesk.

93. Plaintiff then spoke with a Change Healthcare representative for about ten minutes, only to be directed back to AlphaScrip for further assistance.

94. Despite contacting AlphaScrip again, as directed by Change Healthcare, Plaintiff was still unable to obtain any information on how to recover his money.

95. Ultimately, Defendants sent Plaintiff on a frustrating and unproductive chase, as every party he was directed to contact disclaimed responsibility for Defendants' failure to process his Savings Card. Instead, he was informed that the issue was entirely due to the Change Healthcare Data Breach and the subsequent system outages.

96. Despite Plaintiff's best efforts, he has not received any reimbursement from Defendants, nor has he been provided with information regarding the reimbursement procedure for the out-of-pocket fees paid when Change Healthcare's systems were offline.

97. Furthermore, Plaintiff did not receive any notice or communication from the Defendants until September 3, 2024, when he was informed by Change Healthcare through a "Notice of Data Breach" that his data may have been compromised. The notice provided details about the potential exposure of personal information and available protective measures, but notably, it failed to mention any impact on Savings Card processing or offer resources for reimbursement or refunds. To date, CVS has failed to provide Plaintiff with any substantive communication about the issue. Plaintiff first became aware of the problem with his Savings Card during his visit to the CVS Pharmacy, where the information provided was vague, incomplete, and failed to offer a clear explanation or effective resolution to the problem.

98. As a direct and proximate result of Defendants' actions and inactions, Plaintiff and Class Members (defined below) have incurred financial harm, having paid out-of-pocket expenses that should have been covered by the Savings Cards during the period when Change Healthcare's systems were offline.

99. Additionally, Plaintiff and Class Members have invested significant time, energy, and money to mitigate the impact of their inability to use their Savings Cards. They have also spent considerable time communicating with insurance companies and pharmacies in an attempt to resolve these issues, all in the face of Defendants' silence.

100. The inability of Defendants to process Savings Cards caused significant hardship to Plaintiff and Class Members, many of whom depend on the discounts provided by the Savings Cards to manage their healthcare needs effectively.

CLASS ACTION ALLEGATIONS

101. Plaintiff brings this action against Defendants on behalf of himself and all other persons similarly situated, pursuant to Rule 23 of the Federal Rules of Civil Procedure.

102. Specifically, Plaintiff seeks to represent a Class, subject to amendment as appropriate, and defined as follows:

All individuals in the United States and its territories who were unable to utilize their Savings Cards at CVS as a result of the Change Healthcare Data Breach that occurred on or around February 21, 2024 and who have not been reimbursed by Defendants for the difference in price of what they paid for their prescription(s) and what they would have paid had they been able to utilize their Savings Cards (the “Class”).

103. Included in this Class is a Subclass of Connecticut residents, subject to amendment as appropriate, and defined as follows:

All citizens of Connecticut who were unable to utilize their Savings Cards at CVS as a result of the Change Healthcare Data Breach that occurred on or around February 21, 2024 and who have not been reimbursed by Defendants for the difference in price of what they paid for their prescription(s) and what they would have paid had they been able to utilize their Savings Cards (the “Connecticut Subclass”).

104. Excluded from the Class are Defendants and Defendants’ parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; and all individuals who make a timely election to be excluded from the Class using the correct protocol for opting out.

105. The proposed Class is defined based on the information available to Plaintiff at this time. Plaintiff reserves the right to modify or amend the definition of the proposed Class and Connecticut Subclass before the Court determines whether certification is appropriate.

106. Numerosity. Members of the Class (“Class Members”) and Connecticut Subclass Members are so numerous that joinder of all Class Members and Connecticut Subclass Members is impracticable. Upon information and belief, there are at least thousands of individuals who were

unable to benefit from the use of their Savings Cards at CVS due to the Data Breach, which resulted in Change Healthcare shutting down its systems.

107. Commonality. Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

- a. Whether Defendants failed to implement and maintain reasonable procedures and practices to allow for the processing of Savings Cards in the event of a data breach;
- b. Whether Defendants were negligent in failing to process Savings Cards following the Data Breach;
- c. Whether the Defendant CVS's failure to process Savings Cards constituted a breach of its contractual obligations to the Plaintiff and the Class, thereby causing financial harm to the Plaintiff, the Class, and the Connecticut Subclass.
- d. Whether Defendants took reasonable measures to reinstate the processing of Savings Cards following the Data Breach;
- e. Whether Defendants response to the Data Breach was reasonable;
- f. Whether Defendants had adequate procedures and practices in place to facilitate reimbursements to Class Members following the Data Breach;
- g. Whether the Defendants failure to allow for processing of Savings Cards caused Plaintiff's and the Class's injuries;
- h. What the proper measure of damages is; and
- i. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

108. Typicality. Plaintiff's claims are typical of the claims of the Class Members. The claims of the Plaintiff and Class Members are based on the same legal theories and arise from the

same unlawful conduct. Defendants, Change Healthcare and CVS, were responsible for ensuring the proper functioning of the systems used to process Savings Cards at CVS pharmacies.

109. Adequacy of Representation. Plaintiff is an adequate representative of the Class. Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to those of the other Class Members, and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. In addition, Plaintiff has retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

110. Superiority. This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all Class Members is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense, and promote uniform decision-making.

111. Predominance. Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendants' liability and the fact of damages are common to Plaintiff and each Class Member. If Defendants breached their duty to Plaintiff and Class Members, then Plaintiff and each Class Member suffered damages by that conduct.

112. Ascertainability: Class membership is defined using objective criteria and can be readily identified through the records maintained by CVS. CVS can determine Class Members by reviewing their detailed books and records, which include transaction histories for drugs purchased at CVS that were eligible for Savings Cards, as well as records of Savings Card usage. Indeed, Plaintiff's Savings Card is recorded and on file at CVS.

COUNT I - NEGLIGENCE

On Behalf of Plaintiff and the Class Against Change Healthcare

113. Plaintiff restates and realleges the allegations contained in every preceding paragraph as if fully set forth herein.

114. Defendant Change Healthcare owed a duty of care to Plaintiff and Class Members because it was responsible for managing and maintaining critical healthcare systems that directly affected consumers' ability to access medication discounts through Savings Cards. As the entity controlling these systems, the harm to consumers from system outages was entirely foreseeable and inevitable. Specifically, Change Healthcare knew or should have known that interruptions to the processing of Savings Cards would result in direct harm to consumers who use these discounts to afford their essential medications. Specifically, Change Healthcare knew or should have known that interruptions in Savings Card processing would lead to significant financial hardship for consumers.

115. Change Healthcare's duty of care further arose from its integral function within the healthcare ecosystem. The operational continuity of its systems is crucial to ensuring access to important services like Savings Cards. In light of known risks, such as data breaches, it was reasonably foreseeable that any interruptions or failures in maintaining these systems would lead to direct harm, depriving consumers of the financial relief they were entitled to when purchasing

medications. Given the foreseeable risk and severity of harm, Change Healthcare had a duty to implement reasonable safeguards, especially in the face of predictable threats like the Data Breach.

116. Change Healthcare breached its duty by failing to implement reasonable preventive measures, such as developing robust contingency plans and offering alternative methods to ensure the processing of Savings Cards during foreseeable system disruptions. These measures were practical, feasible, and aligned with industry standards. Furthermore, the burden of implementing these measures was minimal compared to the significant harm consumers faced. Change Healthcare's failure to take such reasonable precautions significantly increased the risk of harm to consumers, denying them access to the financial relief they would otherwise have received for medications.

117. Change Healthcare's duty to implement preventive measures is also grounded in its regulatory obligations. As a HIPAA-covered entity, Change Healthcare is required to establish contingency plans to ensure the availability and integrity of ePHI during emergencies, such as system failures or data breaches. This obligation to protect ePHI reflects a broader expectation that Change Healthcare must also maintain critical operational functions, like Savings Card processing, which directly affect consumers.

118. Change Healthcare's duty to implement preventive measures is further supported by industry standards, such as those outlined in the NIST Special Publication 800-53 Revision 5, Security and Privacy Controls for Federal Information System and Organization ("NIST 800-53"). These guidelines, while not legally binding, are widely recognized in healthcare for managing critical systems. NIST emphasizes the necessity of robust contingency planning, including the development of backup systems, incident response protocols, and alternative processing capabilities, especially in the face of foreseeable risks like data breaches.

119. Despite foreseeable risks, Change Healthcare failed to implement adequate contingency measures and alternative solutions to ensure Savings Card processing during the Data Breach. This breach of duty directly resulted in financial harm to Plaintiff and Class Members, who were unable to access medication discounts that they reasonably expected to be available. Tennessee law recognizes that defendants may be held liable for injuries resulting from their failure to foresee and mitigate risks. In this case, the causal link between Change Healthcare's system outage and the consumers' financial losses is direct and unavoidable. Plaintiff and Class Members suffered tangible financial harm, which was foreseeable and preventable.

120. As an experienced technology provider in the healthcare space, Change Healthcare was fully aware of the necessity for robust contingency plans to ensure operational continuity. Its failure to uphold these duties, and refusal to address the financial harm caused, resulted in significant economic losses to Plaintiff and Class Members. The company had ample opportunity to foresee the potential consequences of a system failure, particularly given the well-known risk of data breaches. The failure to plan appropriately for these foreseeable events breaches the duty of care required of an entity managing critical healthcare systems.

121. As a direct and proximate result of Change Healthcare's negligence, Plaintiff and Class Members have suffered injury. This includes financial harm from being unable to use their Savings Cards and the additional burden of not being reimbursed for the discounts they were denied. Change Healthcare's actions have caused substantial economic losses and hardship for Plaintiff and Class Members. Tennessee law holds defendants liable for injuries when their negligence is a substantial factor in causing harm, and in this case, the direct causal chain between Change Healthcare's breach and the financial losses sustained by Plaintiff and Class Members satisfies both proximate and actual causation.

COUNT II - BREACH OF CONTRACT (THIRD-PARTY BENEFICIARY)

On Behalf of Plaintiff and the Class Against Change Healthcare

122. Plaintiff restates and realleges the allegations contained in every preceding paragraph as if fully set forth herein.

123. Defendant Change Healthcare entered into contracts with CVS to provide technology services, including billing, processing, and other administrative functions integral to CVS's operations. An aspect of these services included the processing of Savings Cards, which directly impacted CVS's ability to fulfill its commitments to consumers.

124. The contractual relationship between CVS and Change Healthcare was intended to support CVS's implied-in-fact contract with Plaintiff and Class Members, which arose from CVS's conduct, advertisements, and representations that it would honor Savings Cards for medication discounts. This implied contract established consumer expectations that CVS and, by extension, Change Healthcare, would process these discounts.

125. Plaintiff and Class Members are third-party beneficiaries of the contract between CVS and Change Healthcare, as the performance of this contract was critical to fulfilling CVS's implied obligations to consumers. The functionality and reliability of Savings Card processing were essential components of the benefits Plaintiff and Class Members expected to receive.

126. Change Healthcare breached its contractual obligations by failing to maintain operational continuity, failing to implement adequate contingency measures, and failing to protect its systems against foreseeable disruptions, such as data breaches. These breaches directly interfered with CVS's ability to fulfill its implied-in-fact contractual obligations to Plaintiff and Class Members.

127. Moreover, despite having the opportunity to reimburse Plaintiff and Class Members for the financial harm caused by the inability to process Savings Cards, Change Healthcare failed to take corrective action or provide any compensation for the discounts lost due to its breaches.

128. As a result of Change Healthcare's breach, Plaintiff and Class Members were deprived of the discounts promised under the implied contract with CVS, causing them to suffer financial harm, including out-of-pocket payment for medications at full price.

129. Change Healthcare's breach not only violated its contractual duties to CVS but also undermined the reasonable expectations of Plaintiff and Class Members as third-party beneficiaries. As a direct and proximate result of Change Healthcare's failure, Plaintiff and Class Members incurred significant financial losses.

130. Plaintiff and Class Members seek compensation for these damages, including the difference between the discounted price they were led to expect and the full price they were forced to pay, and any other relief deemed appropriate by the Court.

COUNT III - NEGLIGENCE

On Behalf of Plaintiff and the Class Against CVS

131. Plaintiff restates and realleges the allegations contained in every preceding paragraph as if fully set forth herein.

132. Defendant CVS owed a duty of care to Plaintiff and Class Members to ensure the continuous and reliable processing of Savings Cards at its pharmacies. This duty is rooted not only in CVS's public and private representations but also from the reasonable expectations CVS deliberately fostered through advertising, marketing, and its routine acceptance of Savings Cards for prescription discounts.

133. CVS's advertising, signage, and consistent communications explicitly stated that it accepted Savings Cards for prescription discounts. Indeed, it regularly kept customers Savings

Cards on file as it did with Plaintiff's Savings Card. These representations were actionable commitments designed to attract and retain customers. By consistently representing that it would honor Savings Cards, CVS induced Plaintiff and Class Members to reasonably expect that they could rely on CVS for these discounts and thus owed a duty to exercise reasonable care in maintaining systems that could reliably process Savings Cards.

134. Data breaches and system outages are foreseeable risks within the healthcare and retail industries. CVS knew or should have known that system disruptions, such as those caused by data breaches, were foreseeable and could directly impact its ability to fulfill its advertised commitments to customers. As such, CVS had a duty to take reasonable precautions, including the implementation of alternative processing methods, manual overrides, or timely notifications to consumers about potential impacts on their ability to use Savings Cards.

135. CVS's promotion of the Savings Cards, along with its practice of storing these cards on file, created a reasonable expectation among customers that their Savings Cards would be processed as represented. This expectation was a foreseeable and intended consequence of CVS's marketing and operational practices. Accordingly, CVS had a duty to ensure that its systems were equipped to meet these expectations, particularly during disruptions such as the Data Breach.

136. CVS also had a broader duty stemming from its implied contractual obligations to ensure the continuous processing of Savings Cards, particularly when Savings Cards were promoted as a key benefit. This duty extended to implementing safeguards and contingency measures to protect against foreseeable disruptions in the systems it relied upon, including those managed by Change Healthcare.

137. As a healthcare provider, CVS has a well-established duty of care that extends to maintaining operational reliability, especially in areas impacting consumer health and financial

well-being. While HIPAA regulations specifically mandate contingency planning for ePHI, the principles behind these requirements highlight a broader expectation that CVS must maintain critical business functions during disruptions. Although HIPAA does not directly regulate Savings Card processing, these principles reinforce CVS's duty to maintain reliable service, particularly when it advertises these savings as an essential feature of its offerings, and maintains these Savings Cards on file.

138. Despite knowing the critical reliance on Change Healthcare's systems and the foreseeable risk of unavailability, CVS failed to implement any meaningful contingency plan or alternative methods for processing Savings Cards. Consequently, when Change Healthcare's systems were rendered inoperative due to the Data Breach, CVS was left unable to process Savings Cards, depriving Plaintiff and Class Members of their expected medication discounts.

139. As a direct and proximate result of CVS's negligence, Plaintiff and Class Members were forced to incur significant out-of-pocket expenses for their medications. Despite having the opportunity to reimburse customers for these losses, CVS failed to take corrective action, compounding the financial harm. Plaintiff and Class Members are entitled to compensation for their damages, including the difference between the discounted price they were led to expect and the full price they were forced to pay, and any other relief deemed appropriate by the Court.

COUNT IV - BREACH OF IMPLIED CONTRACT
On Behalf of Plaintiff and the Class Against CVS

140. Plaintiff restates and realleges the allegations contained in every preceding paragraph as if fully set forth herein.

141. Plaintiff and Class Members entered into an implied contract with CVS when they sought to use their Savings Cards at CVS locations, relying on CVS's advertisements and consistent past practices of accepting and processing Savings Cards for prescription discounts.

These representations were made explicitly and implicitly at the point of sale, forming a reasonable expectation that CVS would honor the Savings Card.

142. Through its conduct and representations, including keeping customer's Savings Cards on file, CVS expressly and implicitly agreed to honor and process the Savings Cards presented by Plaintiff and Class Members, thereby providing the promised discount on prescription medications. This agreement was not merely a general marketing statement but an actionable commitment tied to the specific transaction at hand.

143. Plaintiff and Class Members entered into the implied contracts with the reasonable expectation that CVS would continue to accept Savings Cards as advertised, and that CVS's systems and procedures were adequate to fulfill its promise of processing these cards. This expectation was supported by CVS's ongoing conduct and consistent course of dealing, including keeping customer's Savings Cards on file, which CVS knew would induce reliance by consumers.

144. Plaintiff and Class Members reasonably relied on CVS's representations and consistent conduct, expecting CVS to uphold its implied promise to process the Savings Cards during their purchases. The ability to use these Savings Cards for discounts was a critical aspect of the implied agreement between the parties.

145. The acceptance of Savings Cards were a critical factor in the Plaintiff's and Class Members' decisions to purchase their medications at CVS, making it a material term of the implied contract between the parties. Plaintiff and Class Members reasonably relied on CVS's consistent and specific representations, both publicly and through past practices, that it would process Savings Cards. This reliance was foreseeable and directly induced by CVS's conduct, which assured customers that their Savings Cards would be honored at the point of sale.

146. Plaintiff and Class Members fully performed their obligations under the implied contracts by either presenting their Savings Cards at the time of purchase or having their Savings Cards stored on file, in accordance with CVS's advertised policies and the reasonable expectations created by CVS's consistent course of conduct.

147. CVS breached these implied contracts when it failed to process the Savings Cards due to the system outage caused by the Data Breach. Despite knowing the critical role of the Savings Card in the customer's decision to purchase medications at CVS and the foreseeable risk of system failures, CVS did not implement reasonable contingency measures, alternative processing methods, or any backup plan to ensure that Savings Cards would continue to be honored during such outages.

148. Moreover, CVS had the opportunity to reimburse Plaintiff and Class Members for the out-of-pocket costs incurred as a result of its failure to process the Savings Cards but chose not to do so.

149. CVS's breach directly and proximately caused the Plaintiff's damages. The failure to process the Savings Card and CVS's subsequent refusal to reimburse Plaintiff deprived Plaintiff of the benefits of the implied contract, forcing Plaintiff to pay full price for medications that would have been significantly discounted.

150. The injuries sustained by Plaintiff and Class Members due to CVS's breach include financial losses from paying full price for medications that would not have been incurred if CVS had fulfilled its contractual obligations.

151. As a direct and proximate result of the breach, Plaintiff and Class Members are entitled to compensation for their damages, including the difference between the discounted price

they were led to expect and the full price they were forced to pay, and any other relief deemed appropriate by the Court.

**COUNT V - VIOLATION OF THE CONNECTICUT UNFAIR TRADE
PRACTICES ACT**

On Behalf of the Connecticut Subclass Against CVS

152. Plaintiff repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

153. The Connecticut Unfair Trade Practices Act (“CUTPA”), Conn. Gen. Stat. § 42-110a et seq., prohibits unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce.

154. CVS engaged in unfair and deceptive practices by misleading Plaintiff and Class Members into believing that their Savings Cards would be honored without issue. CVS’s marketing, signage, and consistent communications created a false expectation that consumers could reliably use their Savings Cards to receive discounts on prescription medications. These practices were not merely accidental but were designed to induce reliance and attract customers to CVS’s services.

155. CVS knew, or should have known, that its systems were vulnerable and that its reliance on compromised processing systems could result in the inability to process Savings Cards. Despite this knowledge, CVS failed to take reasonable steps to prevent or mitigate the impact of this failure, demonstrating a disregard for the rights and expectations of its consumers.

156. CVS’s failure to process the Savings Cards during the relevant period was not due to an unforeseen event but rather a result of CVS’s decision to rely on inadequate systems without implementing necessary contingency measures. This decision was made with the knowledge that

such failures would likely occur and directly prevent Plaintiff and Class Members from receiving the discounts to which they were entitled.

157. CVS's refusal to reimburse Plaintiff and Class Members for the out-of-pocket expenses they incurred further exacerbates the harm caused by its deceptive conduct. CVS had multiple opportunities to mitigate the financial impact on consumers but chose to ignore these responsibilities, further demonstrating an unfair and deceptive pattern of behavior under CUTPA.

158. As a direct result of CVS's failure to address these issues, Plaintiff and Class Members were unable to use their Savings Cards to obtain necessary medications at the discounted prices they were promised, resulting in significant financial harm. This harm was a foreseeable and direct outcome of CVS's conscious decision to prioritize operational convenience over customer protection.

159. The inability to use the Savings Cards forced Plaintiff and Class Members to pay full price for medications, resulting in unexpected economic losses and financial burdens. These individuals relied on the Savings Cards for financial relief, and CVS's failure to process these cards as expected caused substantial out-of-pocket expenses.

160. Plaintiff and Class Members have suffered actual damages, including the difference between the discounted price they expected to pay and the full price they were forced to pay for their medications.

161. CVS's actions constitute trade or commerce under CUTPA, as they involve the provision of services integral to the management of healthcare costs. Conn. Gen. Stat. § 42-110b(d) directs that CUTPA be interpreted and enforced consistently with the Federal Trade Commission Act, 15 U.S.C. § 45(a)(1), which prohibits unfair or deceptive acts or practices.

162. Under Conn. Gen. Stat. § 42-110g(a), Plaintiff and Class Members are entitled to bring an action to recover actual damages. Moreover, if the Court finds that the violation was willful or knowing, Plaintiff and Class Members may be awarded punitive damages, attorneys' fees, and costs.

163. By failing to implement reasonable contingency plans, failing to reimburse customers, and misleading consumers about the reliability of Savings Card processing, CVS engaged in conduct that was both deceptive and unfair under CUTPA.

164. Plaintiff and Class Members seek compensation for the economic losses suffered due to Defendants' violations of CUTPA, including reimbursement for out-of-pocket expenses and any additional relief deemed appropriate by the Court to address CVS's unfair and deceptive practices.

COUNT VI - BREACH OF THE TENNESSEE CONSUMER PROTECTION ACT OF
1977

On Behalf of Plaintiff and the Class Against CVS

165. Plaintiff restates and realleges the allegations contained in every preceding paragraph as if fully set forth herein.

166. The Tennessee Consumer Protection Act of 1977 ("TCPA"), Tenn. Code § 47-18-104(a), declares that "[u]nfair or deceptive acts or practices affecting the conduct of any trade or commerce constitute unlawful acts or practices."

167. Tenn. Code § 47-18-109 provides a private right of action for violations of the law, stating that "[a]ny person who suffers an ascertainable loss of money . . . as a result of the use or employment by another person of an unfair or deceptive act or practice . . . may bring an action individually to recover actual damages." Moreover, if a violation is "willful or knowing . . . the court may award three (3) times the actual damages sustained and may provide such other relief as it considers necessary and proper."

168. The Tennessee Supreme Court clarified that the TCPA applies to business practices of healthcare providers, not just their professional services. The Court held that “when a plaintiff alleges an injury caused by a health care provider’s business practices—including, but not limited to, deceptive practices in advertising, billing, or collections—the plaintiff may state a claim under the TCPA.”⁴⁶

169. Defendant CVS engaged in unfair and deceptive practices by misleading Plaintiff and Class Members into believing that their Savings Cards would be reliably honored as advertised. CVS’s public and private representations, including advertising and direct communications, were intended to assure consumers that they would benefit from these discounts, and such assurances were central to attracting and retaining customers.

170. CVS’s assurances about the acceptance of Savings Cards were deceptive, violating the TCPA’s prohibition on creating false impressions about the availability of services (Tenn. Code Ann. § 47-18-104(b)(7)). By promoting itself as a reliable participant in the Savings Card program, CVS induced consumer trust without disclosing significant vulnerabilities in its processing systems or its lack of contingency plans.

171. CVS’s failure to process the Savings Cards during the relevant period was not due to an unforeseeable event but a direct result of CVS’s decision to rely on inadequate systems without implementing alternative processing methods or backup plans. CVS knew or should have known that such failures would significantly impact consumers who depended on these advertised discounts to manage the costs of their medications.

⁴⁶ *In re Investigation of Law Sols. Chi. LLC*, 629 S.W.3d 124, 126 (Tenn. Ct. App. 2021)

172. Moreover, CVS failed to take corrective action after the disruption occurred. It had the opportunity to refund consumers or honor the discounts retroactively, but instead chose not to, compounding the financial harm to Plaintiff and Class Members.

173. CVS's actions reflect a broader pattern of prioritizing its operational convenience over consumer protection. By failing to address vulnerabilities in its systems, refusing to implement basic contingency measures, and failing to notify consumers of potential disruptions, CVS demonstrated a reckless disregard for the rights and expectations of its customers.

174. As a direct result of CVS's unfair and deceptive practices, Plaintiff and Class Members were unable to use their Savings Cards to obtain necessary medications at the discounted prices they were promised, leading to significant financial harm. This financial harm was foreseeable and directly caused by CVS's failure to uphold its commitments to consumers.

175. The inability to use the Savings Cards forced Plaintiff and Class Members to pay full price for medications, resulting in unexpected economic losses and financial burdens. Plaintiff and Class Members relied on CVS's assurances and advertised commitments, and CVS's failure to uphold these promises caused substantial out-of-pocket expenses that CVS refused to reimburse.

176. Plaintiff and Class Members have suffered actual damages, including the difference between the discounted price they were led to expect and the full price they were forced to pay, resulting in substantial out-of-pocket expenses and financial burdens directly caused by CVS's deceptive conduct.

177. CVS's conduct also violates the TCPA's prohibition against "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have" (Tenn. Code Ann. § 47-18-104(b)(5)). By failing to provide the

promised processing of Savings Cards, CVS misled Plaintiff and Class Members regarding the availability and reliability of these discounts.

178. Plaintiff and Class Members are entitled to recover damages, attorneys' fees, and costs, as provided under the TCPA.

179. The damages suffered by Plaintiff and Class Members include, but are not limited to, the out-of-pocket expenses incurred due to the inability to use Savings Cards, *i.e.*, the difference between the discounted price and the full price of medications, caused by Defendants' unfair and/or deceptive acts.

180. Defendants' failure to uphold their obligations, compounded by its refusal to reimburse affected consumers, and the subsequent harm to Plaintiff and Class Members exemplify a clear violation of the TCPA. Plaintiff and Class Members seek compensation for these damages and any other relief deemed appropriate by the Court.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff demands judgment and relief against Defendants, as follows:

1. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiff is a proper class representative; and appoint Plaintiff's Counsel as Class Counsel;
2. That the Court award Plaintiff and Class Members damages in an amount to be determined at trial;
3. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendants as a result of their unlawful acts, omissions, and practices;
4. That the Court award statutory damages, and punitive or exemplary damages, to the extent permitted by law;

5. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

6. That the Court award pre-judgment and post-judgment interest at the maximum legal rate; and

7. That the Court grant all such other relief as it deems just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

RESPECTFULLY SUBMITTED this October 15th, 2024.

/s/Jerry E. Martin

Jerry E. Martin (TNBPR No. 20193)

Seth M. Hyatt (TNBPR No. 31171)

Barrett Johnston Martin & Garrison, PLLC

200 31st Ave. N

Nashville, TN 37203

(615) 244-2202

Fax: (615) 252-3798

jmartin@barrettjohnston.com

shyatt@barrettjohnston.com

Chet B. Waldman (NYBPR No. 232060) *

Emer Burke (NYBPR No. 5868203) *

Wolf Popper

845 Third Ave.

New York, NY 10022

Telephone: (212) 759-4600

Fax: (212) 486-2093

cwaldman@wolfdpopper.com

eburke@wolfdpopper.com

**Pro Hac Vice Forthcoming*

Attorneys for Plaintiff